云南大学附属医院网络安全改造及等保测评信息化系统采购项目建设需求

一、需求概述

随着信息技术的不断发展和医院智慧化进程的不断推进，数据中心及网络空间安全能否高质量运行变得愈发重要。依据国家相关政策要求，从医院信息系统动态保障的实际需要出发，基于医院的组织架构、管理办法、技术控制和运作机制，遵循相关法律法规，以需求为导向，以风险控制管理、业务连续性服务为理念，按照PPDR和PDCA的思路，建立起可持续性覆盖医院数据中心运行及动态网络空间安全建设全生命周期的信息安全运营体系，开展常态化、闭环化的信息安全运营工作，为云南大学附属医院智慧化背景下的数据中心及信息系统提供立体、纵深的动态安全保障体系。

二、需求内容

目前云南大学附属医院基础数据中心及网络空间安全主要围绕以下五个方面需求展开：

1、依据国家相关政策要求，网络空间安全总体设计指引以“一个中心、三重防护”为理念，从现有的被动防御的安全体系向事前预防、事中响应、事后审计的动态保障体系转变。从安全技术体系、安全管理体系、安全运营体系三方面来实现信息安全建设。建立安全技术体系和安全管理体系，构建具备相应等级安全保护能力的网络安全综合防御体系，开展组织管理、机制建设、安全规划、通报预警、应急处置、态势感知、能力建设、监督检查、技术检测、队伍建设、安全培训和日常运维保障等工作。

2、构建完整的数据中心及动态网络空间运行质量洞察运维管理体系方案，从IT基础设施运行态势管理，包括在资源层面构建业务为导向的可视化安全运维管理，多维度可视化视图管理，到核心业务运行态势可视化管理；以及处理安全事件有效的记录手段，形成体系，逐步建立起精细化、主动式、可视化、流程化、标准化、一体化、智能化的IT运维管理体系，基于智慧医院业务运行背景优化现有运维体系，建立符合数据中心实际情况的运维管理流程及运维体系，提高运维效率。掌握IT设施的运行趋势，安全趋势、资源运行态势、业务运行态势、提高IT资源、业务应用、数据存储的安全性；预判业务系统整体健康状况和运行趋势，从而有效保障业务应用的连续运行。

3、依据《全国医院信息化建设标准与规范（试行）》规范要求，构建整体信息化业务系统的安全性、业务连续性保障体系方案。通过技术与管理手段的结合，设计一套完整的灾备系统管理体系，规范灾备系统的应用流程、提升综合管理水平、降低业务安全风险、减轻运维压力，达到医院智慧医院背景下对于信息化业务系统的各项安全灾备指标。同时，帮助医院在相关各项政策、标准、要求中灾备相关的标准实现与达成，包括但不限于ISO27001、网络安全等级保护制度、灾难恢复规范等。

4、提供数据中心运行及动态网络空间全域安全持续监测、发现、预警、防护运维服务，及时提出有效应对解决方案并组织甲方协同处理可能存在的网络安全威胁；基于基础数据中心全局视角、保障系统健康稳定运行；对业务变更、技术革新、新系统测试、上线、生命周期等全局集成性工作提供及时专业支持。

5、按事件、巡检结果、月度分析可能对医院业务系统和IT系统的安全性造成威胁的各种风险因素并提出相应的对策和改进方案。风险分析的工作将不仅仅只是提出补救措施，还将定义出对于风险的预防措施。

6、汇集数据中心运行及动态网络空间全域事件及机器数据，构建多域机器数据及事件全生命周期管理；提升全域数据应用能力，逐步实现以数据驱动信息平台运营。

**产品清单附表（产品类）：**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **规格要求** | **数量** | **单位** |
| 1 | 下一代防火墙 | 2U机箱，单电源，标配≥16个千兆电口，≥4个千兆光口插槽，内置≥64G SSD硬盘，整机吞吐量≥20Gbps，入侵防御（IPS）吞吐量≥5Gbps，并发连接数≥400万，每秒新建连接数≥5万条/秒，IPSec VPN隧道数≥20000条，默认提供200个SSL VPN用户并发许可；支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路；支持基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路；支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。支持一体化安全策略配置，可以通过一条策略实现用户认证、入侵防御、数据防泄漏、防病毒、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。支持漏洞扫描功能，可实现对包括但不限于后门、服务探测、文件共享、Windows系统补丁、认证等进行主动式扫描，并支持一次性、周期性定时等扫描策略设置。支持Web攻击防护功能，可实现对SQL注入攻击、XSS跨站脚本攻击、Webshell恶意上传行为，以及弱口令、版本探测、漏洞扫描行为等的攻击防护。系统应具备抗拒绝服务攻击能力，基于专业高效的攻击防护算法，实现对主流ICMPFLOOD、SYNFLOOD、ACKFLOOD、SYNACKFLOOD、UDPFLOOD等拒绝服务攻击防护。提供入侵防护、防病毒模块，提供三年入侵防御IPS特征库和三年防病毒AV特征库升级服务；提供三年设备维保服务。 | 1 | 台 |
| 2 | 防火墙 | 2U机架式设备，标配≥20个千兆电口，≥4个千兆光口插槽，内置≥64G SSD硬盘，整机吞吐量≥20Gbps，入侵防御（IPS）吞吐量≥5Gbps，防病毒（AV）吞吐量≥3Gbps，应用层（IPS+AV+ACM）吞吐量≥2Gbps，并发连接数≥400万，每秒新建连接数≥4万条/秒，IPSec VPN隧道数≥20000条，提供≥200个SSL VPN用户并发许可；支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路；支持基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路；支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。支持一体化安全策略配置，可以通过一条策略实现用户认证、入侵防御、数据防泄漏、防病毒、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。支持漏洞扫描功能，可实现对包括但不限于后门、服务探测、文件共享、Windows系统补丁、认证等进行主动式扫描，并支持一次性、周期性定时等扫描策略设置。支持Web攻击防护功能，可实现对SQL注入攻击、XSS跨站脚本攻击、Webshell恶意上传行为，以及弱口令、版本探测、漏洞扫描行为等的攻击防护。系统应具备抗拒绝服务攻击能力，基于专业高效的攻击防护算法，实现对主流ICMPFLOOD、SYNFLOOD、ACKFLOOD、SYNACKFLOOD、UDPFLOOD等拒绝服务攻击防护。提供三年设备维保服务。 | 1 | 台 |
| 3 | 互联网安全网关 | 2U设备，冗余电源，内置≥64G SSD硬盘，标配≥18个千兆电口，≥4个千兆光口插槽，≥4个万兆光口插槽，≥2个扩展槽位，整机吞吐量≥40Gbps，IPS吞吐量≥6Gbps,防病毒吞吐量≥6Gbps，应用层吞吐量≥8Gbps，最大并发连接数≥1000万，每秒新建连接数≥18万，支持IPSec VPN隧道数≥20000，提供≥200个SSL VPN用户并发许可，支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路；支持基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路；支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。支持一体化安全策略配置，可以通过一条策略实现用户认证、入侵防御、数据防泄漏、防病毒、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。支持漏洞扫描功能，可实现对包括但不限于后门、服务探测、文件共享、Windows系统补丁、认证等进行主动式扫描，并支持一次性、周期性定时等扫描策略设置。支持Web攻击防护功能，可实现对SQL注入攻击、XSS跨站脚本攻击、Webshell恶意上传行为，以及弱口令、版本探测、漏洞扫描行为等的攻击防护。系统应具备抗拒绝服务攻击能力，基于专业高效的攻击防护算法，实现对主流ICMPFLOOD、SYNFLOOD、ACKFLOOD、SYNACKFLOOD、UDPFLOOD等拒绝服务攻击防护。具备防病毒、入侵防护、上网行为管理等功能，提供三年入侵防御IPS特征库、防病毒AV特征库升级服务。提供三年设备维保服务。 | 2 | 台 |
| 4 | 数据库审计 | 2U机架式设备,双电源，标配≥6个千兆电口（含1个管理口，1个HA口），≥4个千兆SFP光口插槽，支持≥2个扩展槽位，硬盘≥2T\*3，RAID5，有效存储容量≥4T，可审计流量≥800Mbps,入库速度≥32000条/秒，日处理事件数≥5亿条，提供无限个被审计DB服务数，提供防统方许可，支持对Oracle、SQL-Server、DB2、Informix、Sybase、MySQL、PostgreSQL、Teradata、Cache、MongoDB、Redis、分布式数据库Gauss和ES等进行审计，且支持人大金仓KingBase、神通(OSCAR)、达梦(DM)、南大通用(GBase)等国产数据库审计。提供三年设备维保服务。 | 1 | 台 |
| 5 | 运维审计 | 2U机架式设备，6个千兆电口，2个扩展插槽，8G内存，硬盘容量2T，字符并发：1000个，图形并发：300个。提供400点被管理资源数；提供三年设备维保服务。支持资源制定不同改密分组，执行周期性、手动改密操作，改密类型支持：Linux类，国产操作系统中标麒麟，银河麒麟，网络设备（华为、华三、思科、中兴），Windows类，数据库类（Oracle、PostgreSQL、MySql、DB2、Informix 、SYBASE，Mssql等）。为满足等级保护关于身份鉴别-双因素认证的合规要求，本次配置10个动态口令卡实现第二种身份认证方式。 | 1 | 台 |
| 6 | 下一代防火墙 | 2U设备，冗余电源；默认配置一块64G SSD硬盘，标配8个千兆电口，4个千兆光口，4个万兆光口，2个扩展槽位；支持IPSec VPN隧道数：20000，默认含200个SSL VPN用户并发许可；整机吞吐量：80Gbps，IPS吞吐量：60Gbps，防病毒吞吐量：60Gbps，应用层吞吐量：18Gbps，最大并发连接数：1000万，每秒新建连接数：18万；提供入侵防护、防病毒模块，提供三年入侵防御IPS特征库和三年防病毒AV特征库升级服务；支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路；支持基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路；支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。支持一体化安全策略配置，可以通过一条策略实现用户认证、入侵防御、数据防泄漏、防病毒、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。支持漏洞扫描功能，可实现对包括但不限于后门、服务探测、文件共享、Windows系统补丁、认证等进行主动式扫描，并支持一次性、周期性定时等扫描策略设置。支持Web攻击防护功能，可实现对SQL注入攻击、XSS跨站脚本攻击、Webshell恶意上传行为，以及弱口令、版本探测、漏洞扫描行为等的攻击防护。系统应具备抗拒绝服务攻击能力，基于专业高效的攻击防护算法，实现对主流ICMPFLOOD、SYNFLOOD、ACKFLOOD、SYNACKFLOOD、UDPFLOOD等拒绝服务攻击防护。提供三年设备维保服务。 | 2 | 台 |
| 7 | 综合威胁分析一体机系统 | 标准2U机架式设备，冗余电源，提供4个千兆电口，2个万兆SFP+接口（含2个多模光模块），支持≥6个可用扩展槽位，内存≥96G，硬盘容量≥32T，网络层吞吐量≥30Gbps，应用层吞吐量≥10Gbps，最大并发连接数≥50w，每秒新建连接数≥2.5w条/秒。提供三年算法模块升级（包括但不限于：特征规则模块、病毒引擎模块、检测算法、静态检测和动态检测升级等）；应具备网络资产感知分析能力，可配置多级资产分组，支持自动发现网络资产配置，可编辑资产的类型、标签、系统、位置、服务等信息；支持发现失陷资产，支持基于SMB攻击行为、蠕虫传播行为、其他内网攻击以及用户手动确认攻击成功事件分析失陷主机，可以查看主机失陷判定事件的判定性质和处理流程；支持对单资产进行分析并基于时间轴展示资产受到攻击的全部事件。应具备威胁处置能力，支持与网内的日志审计、WAF、防火墙等产品实现协防配合；提供事件帮助知识库，可根据事件名称查看对应事件的详细信息，包括事件名称、安全类型、事件描述、CVE、CNCVE、CNNVD、漏洞发现时间、事件性质判定、事件处理流程等信息；支持配置白名单，可添加IP、域名、MD5、事件名称，在各视角、有效性分析页面可以进行一键加白；支持指定IP和事件关联加白。提供三年设备维保服务。 | 1 | 台 |
| 8 | 态势感知平台系统 | 基本软件包：系统采用了大数据技术，内置分布式非关系型数据库和传统关系型数据库，提供弹性扩展能力和数据高可靠冗余存储。利用流量行为基线，关联分析，特征检测，文件检测、机器学习等多种分析技术，提供网络安全综合分析能力，功能包含平台框架，提供资产分析与管理，脆弱性感知，威胁感知，检索中心，情报分析，运行监控等安全分析功能，同时提供告警中心，策略中心，系统管理，知识库等安全运维功能。内置性能采集器，日志采集器，提供2300个管理节点授权。态势总览：支持对全网安全信息和系统运维处置的综合展示，全网安全信息包括资产安全、运行状况、攻击趋势、脆弱性概况等；系统运维处置包括告警处置，工单处理，闭环处置率统计等提供3年的产品维护升级服务。态势感知软件包部署环境（服务器或虚拟机）推荐：Intel 至强16核以上CPU，128GB以上内存 ，8TB以上可用磁盘空间。 | 1 | 套 |
| 9 | 终端安全管理系统 | 产品形态为软件，软件管理中心安装硬件环境推荐为Windows2008 R2 X64或Windows2012 R2 X64 操作系统，志强4核以上CPU，16G内存，1T硬盘以上；提供基础管理控制台和桌面运维许可，要求客户端集桌面管理、安全基线、资产管理、终端审计、补丁分发、软件分发、移动存储管理、主机防火墙、准入控制、终端防病毒等功能实现为一体，各功能受服务器策略控制可随时启用或或停用，无需新增或重新部署安装客户端程序；提供防病毒模块；提供1200个被管资源授权许可，提供三年病毒库升级，三年软件升级维护服务。 | 1 | 套 |
| 10 | 数据防丢失及业务连续性保护 | X86硬件主模块。4U机架式设备，36个3.5英寸盘位（最大可配置36块3.5英寸硬盘），标配双路Intel 4210 2.2GHz 10core CPU；配置256GB内存（8\*32GB DDR4内存，剩余9个可用内存插槽）；标配2\*480G SSD盘做系统盘,7\*12TB SAS硬盘；标配2个千兆网络端口和2个万兆光口（含光模块）；空闲2个PCI扩展槽（支持8GB或16GB FC HBA卡，1GE或10GE网络接口卡）;企业级副本数据管理软件主模块，包含企业级副本数据管理软件的服务器端和客户端。可通过扩展前端容量或后端容量副本数据管理代理以及其它高级特性模块实现分级数据保护、开发测试数据验证、OLAP应用及大数据应用数据抽取等数据服务功能。软件实施部署，服务器或者主机至少8核16GB，如有重复数据删除等高级特性，或者确保灾备效果，需要根据实际情况适配较高配置，50TB后端容量数据备份代理,企业级副本数据管理软件和副本数据管理一体机按照容量授权模式进行授权的基础容量授权，每一个License含100TB后端数据量备份许可，可扩展搭配其它高级特性license使用。三年售后支持服务，提供7\*24小时电话支持、网络远程技术支持、和邮件支持 | 1 | 台 |
| 11 | 等保测评证书 | 对单位的HIS、LIS、EMR、互联网医院平台、体检中心系统三级系统进行备案提交合格的测评报告；1.提供信息化资产梳理、运行状态监控、安全事件分析、威胁流量检测、安全信息通告和处置方案建议等服务。2.通过专业安全扫描工具对用户单位所有包括但不限于操作系统、网络设备和应用系统等IT资源进行漏洞扫描，并输出脆弱性扫描报告，针对高、中、低风险项进行漏洞验证、安全分析和加固建议。3.根据测评报告针对网络安全等级保护对象（信息系统）存在且可处理的高、中、低风险项进行风险补偿、配置优化和策略调整，采用专业的主机加固工具提供主机安全基线扫描、加固和防护服务。4.构建网络安全人才培养机制，面向单位全体职工提供网络安全意识培训、个人和单位安全防范知识普及服务，面向信息技术人员提供专业的技术培训，包括但不限于安全基础知识体系、安全设备操作配置、安全运维分析和安全事件处置等内容。 | 1 | 项 |
| 12 | 核心交换机 | 最大交换容量≥23Tbps，最大包转发率≥1620Mpps；支持电源模块≥2个，配置双交流电源；配置万兆SFP+端口≥48个，配置QSFP端口≥2个，风扇模块槽位≥2个，扩展插槽≥2个；支持防火墙板卡，支持VxLAN特性；支持IPv6 支持等价路由、VRRP、OSPFv1/v2、OSPF v3、BGP、ISIS 等增强三层路由协议；支持 MCE、MPLS L2VPN、 MPLS L3VPN、VPLS；要求单台配置：配置原装万兆多模光模块≥48个+2个40G光模块； 配置设备原厂维保≥3年。 | 2 | 台 |
| 13 | 服务器 | 配置：配置≥2颗(16C,3.2GHz)）处理器，最多支持2颗英特尔® 至强®Ice Lake系列可扩展处理器；配置≥256GB DDR4内存，内存保护支持ECC、内存镜像、热备支持高级内存纠错等高级功能,最多支持24个内存插槽，最高支持DDR4-3200 内存,最大支持8条英特尔®傲腾™ 数据中心级持久内存；配置≥12块1.92TB SSD SAS 硬盘单元(2.5") ，可支持12块3.5寸硬盘或25块2.5寸SAS/SATA/SSD硬盘；高性能阵列卡，支持RAID0、1、5；配置≥6个USB3.0接口，2个VGA串口；配置≥4口千兆系统集成网卡,4口万兆含模块，独立管理网口；支持网络唤醒，网络冗余，负载均衡等网络高级特性，支持I/O AT加速技术,另外可支持FLOM技术，选择集成双千兆、双万兆等功能；I/O插槽：可支持5个PCIE插槽，支持1个Raid Mezz卡，最多支持4个单宽GPU；配置≥热插拔电源 1+1 冗余，支持550W/800W/1300W铂金电源；内嵌服务器智能管理芯片，可实现完整的IPMI 2.0远程系统监控、远程KVM、虚拟媒体等各种管理功能；支持后续windows server版服务器操作系统安全增强系统软件，从系统层对操作系统进行加固的系统安全；三年免费质保服务。 | 1 | 台 |
| 14 | 数据中心改造 | 1.数据中心机房网络跳线、光纤跳线、设备电源线整理；2.数据中心机房网络跳线、光纤跳线、设备、设备电源线标签制作及张贴；3.数据中心机房线缆敷设及绑扎；4.数据中心机房两端标签制作标签及张贴； | 1 | 套 |
| 15 | 综合布线 | 1、排查数据中心机房及网络设备使用情况，完成日常网络报修和桌面支持业务，1.网络跳线、光纤跳线、设备电源线整理，保障设备信息化服务的正常有序开展。2、数据中心机房（弱电间）20间和内部线路运维、梳理并打标贴，形成详细的网络管理记录，对于发现的问题须现场拍照取证并及时反馈跟进。3、数据中心机房内景区可视化监控设备安全运维，定期汇总常见问题的解决方案，实现景区监控服务台节约集约聚合运用。 | 1 | 套 |
| 16 | 汇聚交换机 | 交换容量≥756Gbps,最大包转发率≥430Mpps；支持交流或者直流供电，支持电源模块≥2个；配置10/100/1000Base-T自适应以太网端口≥48个，万兆SFP+端口≥6个,扩展插槽≥1个，风扇模块槽位≥2个，满配万兆单模光模块；支持MAC地址规格≥64K，支持OpenFlow 1.3标准；支持VXLAN技术；支持EVPN，支持MACsec 硬件加密，实现MAC层安全加密；支持静态路由、RIPv1/v2、RIPng、OSPFv1/v2/v3、BGP4、BGP4+ for IPv6、IS-IS、IS-IS v6、VRRP、VRRP v3；支持防火墙插卡；支持内置AC（无线控制器）功能；符合IEEE 802.3az（EEE）节能标准，支持端口休眠，节省能源；配置双交流电源，配置风扇模块≥2块，配置设备原厂维保≥3年。 | 2 | 台 |
| 17 | 隔离防火墙 | 1U机箱，单电源，标配≥6个千兆电口，≥4个千兆光口插槽，内置≥64G SSD硬盘，整机吞吐量≥40Gbps，入侵防御（IPS）吞吐量≥3Gbps，并发连接数≥400万，每秒新建连接数≥5万条/秒，IPSec VPN隧道数≥20000条，默认提供200个SSL VPN用户并发许可；支持基于应用的策略路由，可实现为不同的应用类型智能选择相应的链路；支持基于 WEB地址URL的策略路由，可实现将不同类型的网站流量智能分配到不同的链路；支持基于文件类型的策略路由，可实现将预定义或者自定义的文件按照不同的分类进行智能选路。支持一体化安全策略配置，可以通过一条策略实现用户认证、入侵防御、数据防泄漏、防病毒、URL过滤、协议控制、流量控制、并发、新建限制、垃圾邮件过滤、审计等功能。支持漏洞扫描功能，可实现对包括但不限于后门、服务探测、文件共享、Windows系统补丁、认证等进行主动式扫描，并支持一次性、周期性定时等扫描策略设置。支持Web攻击防护功能，可实现对SQL注入攻击、XSS跨站脚本攻击、Webshell恶意上传行为，以及弱口令、版本探测、漏洞扫描行为等的攻击防护。系统应具备抗拒绝服务攻击能力，基于专业高效的攻击防护算法，实现对主流ICMPFLOOD、SYNFLOOD、ACKFLOOD、SYNACKFLOOD、UDPFLOOD等拒绝服务攻击防护。提供入侵防护、防病毒模块，提供三年入侵防御IPS特征库和三年防病毒AV特征库升级服务；提供三年设备维保服务。 | 1 | 台 |
| 18 | 服务器安全管理系统 | 提供Windows server端防病毒功能70个点授权，Linux server端防病毒功能40个点授权，提供三年软件升级和授权。支持多引擎协同，可对病毒、木马、恶意软件等进行查杀，提供主动防御功能，针对Linux操作系统进行病毒、木马、恶意软件等进行查杀。提供主动防御功能，系统默认支持主流Linux操作系统。 | 1 | 套 |
| 19 | 终端安全系统 | 产品为软件形态，包含管理控制中心、客户端软件。提供Windows PC端防病毒、补丁管理、主机防火墙、终端管控、移动存储管理、系统加固功能800个点授权，提供三年软件升级和授权。部署环境：管理中心操作系统支持：Windows Server 2012 R2/2016/2019/2022的64位版本（简体中文版）；支持CentOS 7系统。Windows PC操作系统支持：Windows XP\_SP3及以上/Windows Vista/Windows 7/Windows 8/Windows 10/windows 11 | 1 | 套 |
| 20 | 网络核心设备 | 性能满足DNS QPS不低于50万 ，DHCP LPS不低于2500每秒，可管IP容量不低于30万。千兆电口\*2，1GE光口\*4，32G内存，1T硬盘\*2，配置交流冗余电源支持热拔插，内置免维护的高性能数据库，系统应具备系统级、软件功能级冗余备份能力，支持HA部署或负载均衡部署，支撑实现双设备中单一设备故障时的高可用。提供专业的DNS权威/递归解析服务，支持智能解析和业务健康检测调度及同步功能，满足多活、灾备数据中心的解析调度和业务系统横向调度能力。同时提供高性能DHCPv4 / DHCPv6、地址分配和控制、IP准入控制、IP 记录变更、IP 识别、冲突发现、地址回收、审计报表等 IP 管理自动化系统。 | 1 | 套 |
| 21 | 拟态防御系统 | 标准1U机架式设备，双电源，标配≥10个千兆电口，≥4个千兆光口插槽，≥1个串口，≥2个USB接口，硬盘≥128G SSD，网络层吞吐量≥4Gbps，并发连接数≥310万，每秒新建连接数≥4.5万,虚拟终端数量≥2^32个,虚拟网络数量≥1000,虚拟端口数量2^32个；针对网络空间测绘攻击（部署在边界区）：通过拟态防御技术的冗余异构（拟相网络）、移动目标防御技术的动态变幻（拟相服务）、欺骗防御技术的轻交互（拟相主机）实现网络攻击面的动态管理，使得攻击面在每个时间点的呈现都不一样，充满不确定性、不可预测性。进而达到隐藏真实网络结构/业务、混淆攻击的效果，使得网络空间测绘难度指数级增加。针对内网横向移动攻击（部署在业务区）：当攻击者从外部或内部进行端口扫描、渗透攻击时，能够基于动态伪装网络构造技术（拟相网络/拟相主机/拟相服务/微隔离），精准的发现网络中的已知和未知攻击行为。增强主动防御能力，和已有的事中追溯能力、事后安全产品进阶联防联控，形成一个动态闭环的网络安全体系，来加强整体的安全防御能力。提供三年设备维保服务。 | 1 | 台 |
| 22 | 数据范式化系统 | 对不同品牌、类型的安全设备进行数据制定标准化格式，协同安全数据关联分析系统及安全运营处置平台。 | 1 | 项 |
| 23 | 互联网网站监测系统 | 网站安全监测平台致力于web2.0下的应用安全测试和网站安全漏洞的综合扫描分析，其高效准确的安全扫描策略能够准确发现漏洞威胁，并为安全管理人员提供详细专业的漏洞扫描报表。web服务器综合漏洞检测服务覆盖了CVE、packetstorm、OWASP、WebAppSec及国内外安全社区等国际权威安全组织定义的应用程序漏洞。该系统可以全方位的为客户的网站提供安全监测服务，监测内容包括可用性监测、DNS域名解析监测、挂马监测、敏感内容监测等。运营分析师对中高危漏洞进行验证，并结合多种信息对识别的漏洞进行优先级排序，最后提出切实可行的漏洞修复指导。 | 1 | 项 |
| 24 | 安全基线核查系统 | 对相关信息系统包含服务器、数据库、网络设备及安全设备、包括国产化相关IT设施如国产化操作系统、国产化数据库的配置缺陷及恶意代码进行检测，并提供整改建议、输出《安全配置核查报告》 | 1 | 项 |

**动态运营服务清单（服务类）：**

注：所有服务均要求不少于2名具备相关专业认证工程师驻场精细化运营定期完成。

|  |  |  |  |
| --- | --- | --- | --- |
| 综合运行评估服务 | 对基础数据中心及动态网络空间提供以下服务：1、对医院可能面临的主要威胁性风险进行质与量化的评估；2、按照各风险的严重性，分别定义其所处的风险层次和级别；3、根据各风险发生的可能性，分别定义其所处的风险级别；4、定义风险矩阵图、风险分析报告；5、确定合理的减低风险威胁的处理方法和优先次序；6、汇报分析成果和书面报告。7、服务周期：三年 | 1 | 项 |
| 网络空间安全服务 | 1、针对医院包括外网、内网、数据中心区域等网络边界相关安全策略、访问关系、线路连接等情况进行梳理；2、期对数据库异常事件提供审计分析服务对被授权人员和系统的网络操作行为进行解析、分析、记录、汇报；3、动态监测保障跨网数据安全交换的流量安全性，及时预警分析；4、定期对网络主机、操作系统、数据库系统、网络设备、应用系统、常用软件、虚拟化等，并进行漏洞检测、验证、输出报告，提供处置意见汇报，并及时修复有关漏洞及风险；5、定期提供攻击双向特征检测、恶意代码沙箱检测、威胁情报检测、未知威胁检测、丰富的攻击视角分析、ATT&CK分析、全流量报文存储、攻击取证溯源、0day/1day攻击溯源、历史流量重放检测；6、定期提供不少于12个场景的攻击事件分析结果，包括WEB攻击、扫描探测、可疑行为、暴力破解、僵木蠕攻击、DDOS攻击、DNS服务分析、邮件行为分析、挖矿行为、失陷主机分析、攻击链分析、脆弱性分析等，每周输出一份对应的分析报告；及时提供有效的威胁情报信息，并对重要安全事件作出事前预警和防护意见；7、定期对信息系统及相关 提供安全基线核查、资产管理、终端审计、补丁修复、软件分发、移动存储管理、高危指令研判；8、定期提供智慧医院平台、小程序等检测及安全性评估服务，提交报告；9、定期采用自动化渗透测试工具辅助开展渗透测试工作，渗透测试范围应包括操作系统、数据库、应用服务的已知漏洞、不安全配置以及Web应用程序的常见漏洞等；10、提供对即将上线的新业务系统进行专家安全测试，以测试业务系统前端安全防护机制及业务系统本身的业务安全防护情况；11、服务周期：三年 | 1 | 项 |
| 业务连续性灾备服务 | 原厂具备业务连续性灾备服务资质工程师提供风险分析、业务影响分析、分级保护策略评估、可恢复性评估，分解如下：1、对可能面临的威胁及严重性做预判量化评估，并匹配最佳方法论；2、明确医院的关键业务流程，定义各关键业务可容许中断的最大时间长度，明确各关键业务数据丢失的可容许程度；3、定义流程与恢复处置程序，量化明确各信息系统的可靠恢复能力；4、着眼于医院信息系统情况提出最适当的灾难恢复短、中、长期策略；5、服务周期：三年 | 1 | 项 |
| 全域运行事件分析服务 | 1、提供智能化数据管理机制对数据中心设施及网络空间设施全域机器数据及事件进行汇聚集中关联分析，及时研判预警出整个数据中心可能潜在的威胁（分析源不局限于网络安全事件）；2、提供专项采集、集中监控、故障定位、隐患预警、统一展现等具备可观测性的现场服务，直观反馈出整个数据中心关联分析后的业务健康度；3、对全域机器数据及事件持续优化关联分析，逐步形成及时、准确、全面反映与掌握IT运行健康度；4、服务周期：三年 | 1 | 项 |
| 按需联动运维服务 | 1、提供数据中心运行及动态网络空间全域安全持续监测、发现、预警、防护运维服务，及时提出有效应对解决方案并组织甲方协同处理可能存在的网络安全威胁；基于基础数据中心全局视角、保障系统健康稳定运行；对业务变更、技术革新、新系统测试、上线、生命周期等全局集成性工作提供及时专业支持。2、按事件、巡检结果、月度分析可能对医院业务系统和IT系统的安全性造成威胁的各种风险因素并提出相应的对策方案。风险分析的工作将不仅仅只是提出补救措施，还将定义出对于风险的预防措施和整改落实。3、结合业务连续性，对医院所有包括服务器、存储、网络设备、安全设备等IT资产进行月度巡检，及时发现环境、设备、系统、运行等可能存在的问题及隐患，并出具专业的巡检及预警报告进行汇报；4、基于医院数据中心及信息化的全局视角，对业务变更、技术革新、新系统测试、上线、全生命周期保障等相关工作提供及时有效的专业技术咨询、规划设计和建议等支持服务；5、服务周期：三年 | 1 | 项 |
| 巡检服务（每月） | 1.应急演练：准备演练场景，以模拟演练的方式，制定单位建立攻防对抗机制，检验应急预案和应急流程是否完善，提高单位应急处理能力。 2.漏洞扫描服务:采用专业的漏洞扫描工具对本单位信息系统进行安全扫描，发现漏洞，提供扫描报告，并根据扫描报告给出整改建议，包括：服务器、网络设备、安全设备、数据库和应用系统。 3.渗透测试服务:负责汇总技术渗透中发现的安全隐患，应急处理，并使用合规工具进行渗透工作。 4.安全巡检：包括服务器、存储、网络设备、安全设备等。 | 1 | 项 |
| 安全服务（每月） | 1.安全规划与设计服务：为确保本单位信息系统安全，协助本单位对所有信息系统进行整体安全规划，规划内容主要包括信息安全总体架构，信息安全技术体系和信息安全管理体系建设。2.网络防护服务：及时调整各个安全区域的安全策略，确保网络访问安全；及时调整安全设备的安全策略，确保安全策略的有效性；定期分析设备日志，编写安全分析报告。3.安全管理体系规划建设服务：结合本单位信息系统安全需要，建立一套符合信息系统安全等级保护要求的安全管理体系，主要内容包括安全管理机构、安全管理制度、人员安全管理、系统建设管理和系统运维管理等内容。4.安全培训服务：按照本单位要求，提供相应的安全培训，如黑客技术培训、安全加固培训、安全体系政策培训、安全风险意识培训等。5、预防各级信息安全机构网络渗透及相关应对措施。 | 1 | 项 |
| 集成加固 | 包括所有硬件设备的集成、网络架构优化、互联网医院APP加固（2个）、物理环境整改、综合布线、各类耗材、满足等保要求等、 | 1 | 项 |